第54回コンピュータセキュリティ・第1回情報セキュリティ心理学とトラスト合同研究発表会

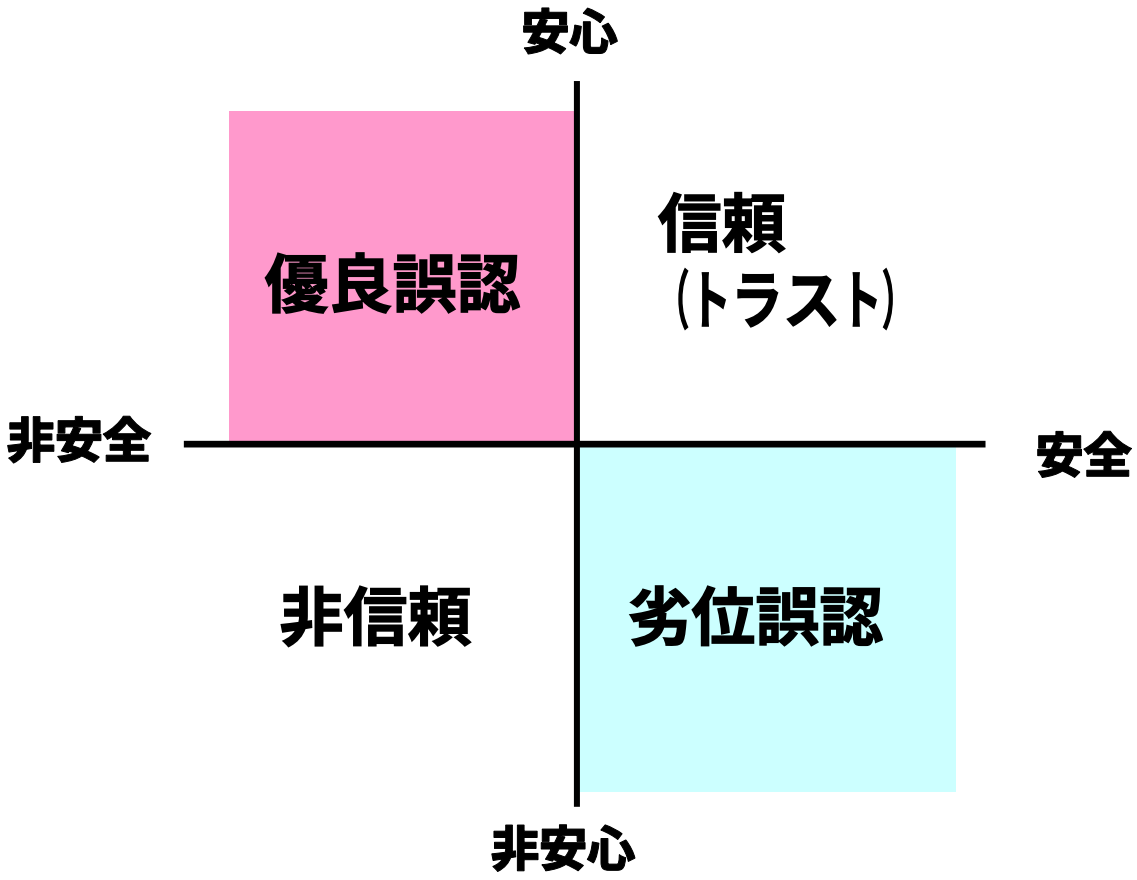
本人認証における信頼の考察

Consideration of Trust in Personal Verification

平成23年7月12日

鵜野幸一郎　　桝野隆平

「安全・安心」の４象限

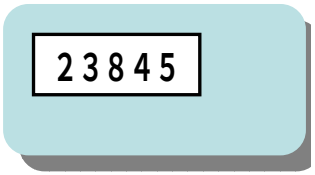


優良誤認　実際は安全でない製品・サービスにも拘わらず安心の心持ちで当該製品・サービスを利用されてしまっている状況を示す象限

劣位誤認　実際は十分安全な製品・サービスであるにも拘わらず，安心感がもてないあまり当該製品・サービスの利用を遠ざけがちになる状況を示す象限

優良誤認（非安全・安心）の例

（1） ワンタイムパスワード



登場時の触れ込み

- パスワード問題を解決する究極のパスワード
- 従来のパスワードを越える最高水準のセキュリティ

＋

ワンタイムパスワードという名称により、本人だけが知る一時的に使うパスワードを連想させる

＋

生成アルゴリズムが高度に専門的であるという利用者の事実認識

⬇

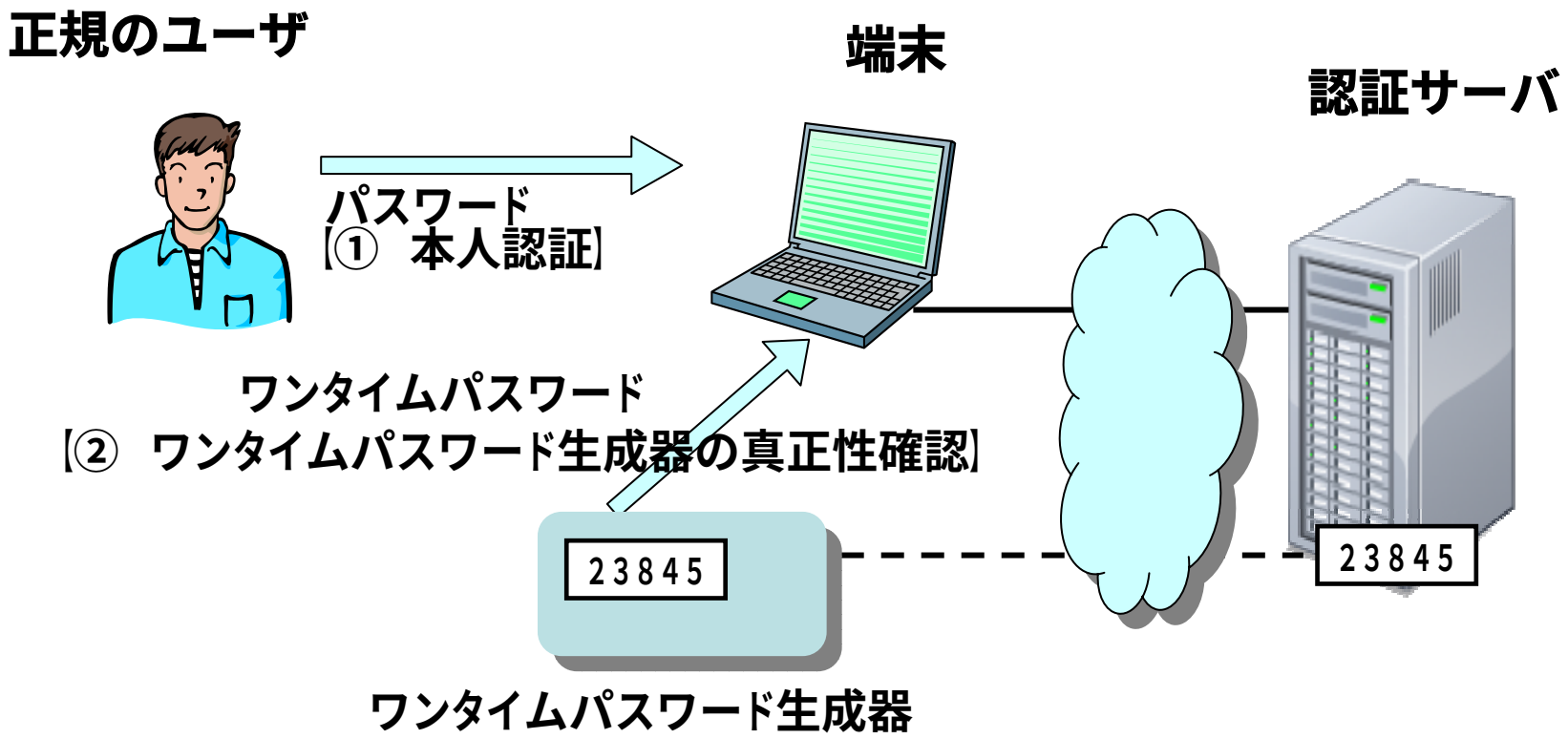
パスワードの上位技術であると思って

なんとなく安心してしまう

(1)　ワンタイムパスワード

ワンタイムパスワードは、あくまでワンタイムパスワード生成器の真正性を証明する機能であり、生成器を所持する当人は誰であっても構わない。

正規のユーザの真正性確認（本人認証）はユーザの記憶している固定パスワードの併用に依存している（2要素法）



(1) ワンタイムパスワード

● 政府機関の認識　本人認証技術の現状に関する調査報告書(IPA　2003.3)

ワンタイムパスワードは、「所持物による認証」である。

▲ 世間一般の認識

ワンタイムパスワードは、「固定パスワードの上位技術」である。

なぜなら、ワンタイムパスワードは、その都度自分で入力するのだからパスワードの一種であり、仮に盗まれても数分後には無効になっているので、盗まれるとその後相当期間に亘って使われてしまう危険性を持つ固定パスワードの限界を破るものだから。

◎ 望ましい名称

「ワンタイムパスワード」ではなく、　**「使い捨てデータ」**

(2)　ＰＫＩないしＰＫＩ搭載ＩＣカード

「PKI搭載ICカードはPKIを搭載しているゆえパスワードの保護なしでもID／パスワードよりも本人認証効果が高い。」との優良誤認の流布 。

1．PKIの定義の専門家と非専門家との差違

「パスワードで保護されたICカードで運用するPKI」を「PKI」と略称する専門家群の存在

「パスワード保護をかける前のPKI」と考える人間が多い非専門家群

2．PKIの魔力的とさえ感じられるセキュリティ技術イメージ定着

パスワード付きPKI搭載ICカードはID／パスワードよりもセキュリティが高いという至極当然の主張　＋　PKI機能に対する過剰な期待

⇨　「PKI」の定義を明確にし情報発信することが学界の課題

(注) ＰＫＩの認証機能にはサーバ認証機能とクライアント認証機能がありますがＰＫＩのクライアント認証におけるクライアントとは、ＰＫＩ機能の搭載されている端末ないしデバイスのこと

（2） ＰＫＩないしＰＫＩ搭載ＩＣカード

「電子署名には送信者は送ったことを否認できなくする機能がある」
と一般に理解されている。　　**（電子書名はＰＫＩ搭載ＩＣカードについては主要な機能の一つ）**

ところが銀行カードと比較してみると、

A **電子署名**　電子署名機能搭載ＩＣカードは正規の利用者に交付されたものであるから利用者は送信行為を否認できない。

B **銀行カード**　ＡＴＭ取引機能搭載銀行カードは正規の預金者に交付されたものであるから預金者はＡＴＭで預金が引き出された結果を否認できない。

Ａが成立するのならばＢも成立してしまいます。Ｂが成立すれば銀行カードを盗まれた預金者は泣き寝入りするしかありません。電子署名の搭載されたＩＣカードが他人によって使われてしまった場合には正規の利用者には否認することが出来ないというのは法理に反し、公序良俗に反するもののように思われます。

ＡもＢも共に利用時には暗証番号で利用者認証をしてカードが正規の利用者の手中にあることを確認させているのでその心配はない、というのならば

「否認を不可能にする」機能を担保しているのは暗証番号であって電子署名ではありません。

(3)　生体認証技術の性能表示の際、本人拒否率(ＦＲＲ)と他人受容率(ＦＡＲ)を独立変数のように扱う

・他人受容率の素晴らしい値だけ表示

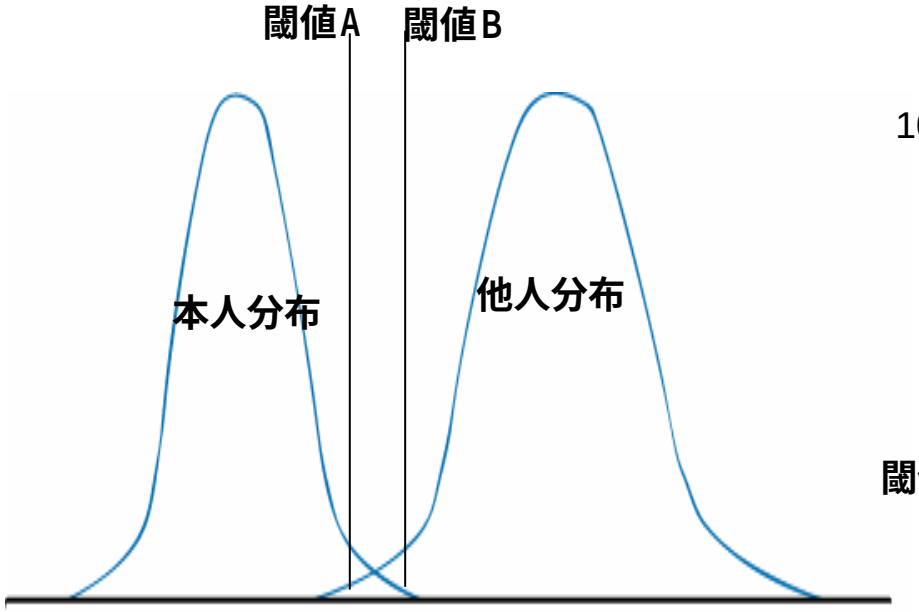
表示例	他人受容率	本人拒否率
片方のみ表示：評価不能	０．０００１％	？
“対”の表示：評価可能	０．０１％	０．１％

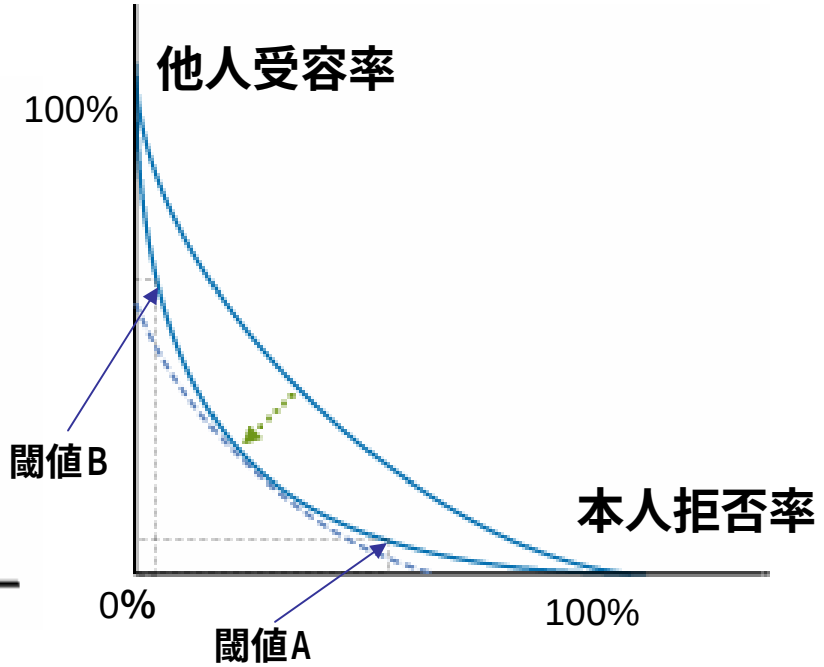
・自社基準値（サンプル数、測定条件など未提示）

➡ 利用者に“生体照合精度”の意味を理解してもらうのは無理というもの。

(3)　生体認証技術の性能表示の際、本人拒否率（ＦＲＲ）と他人受容率（ＦＡＲ）を独立変数のように扱う

【ＦＲＲを高めるとＦＡＲは低くなるというシーソーの関係】





本人分布と他人分布に重なる領域が存在する以上、本人拒否と他人受容も必然的に存在する

他人排除率で妥協しない限りは本人拒否救済策への依存が不可欠

生身の人間を対象とする限り破線のような識別性能向上はありえない。

たとえ精度が向上しても本人拒否率を0%とする閾値では他人受容率は際限なく100%に近づき、他人受容率を0%とすると本人拒否率は100%に近づく。

(4)　安全性を犠牲にして可用性を上げる運用

●　救済用パスワードを併用する生体認証搭載製品

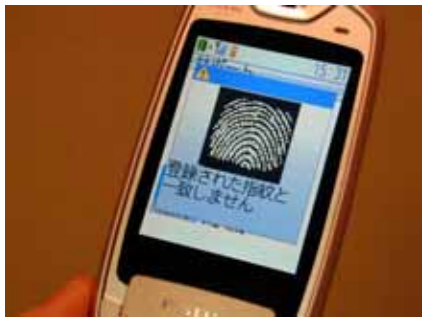
本人認証に関する素朴な質問

暗証番号だけで機密を守る携帯電話A

生体認証装置搭載で『指紋または暗証番号を入力してください。』との表示の出る携帯電話B

どちらのセキュリティ強度が高いですか？

携帯電話A



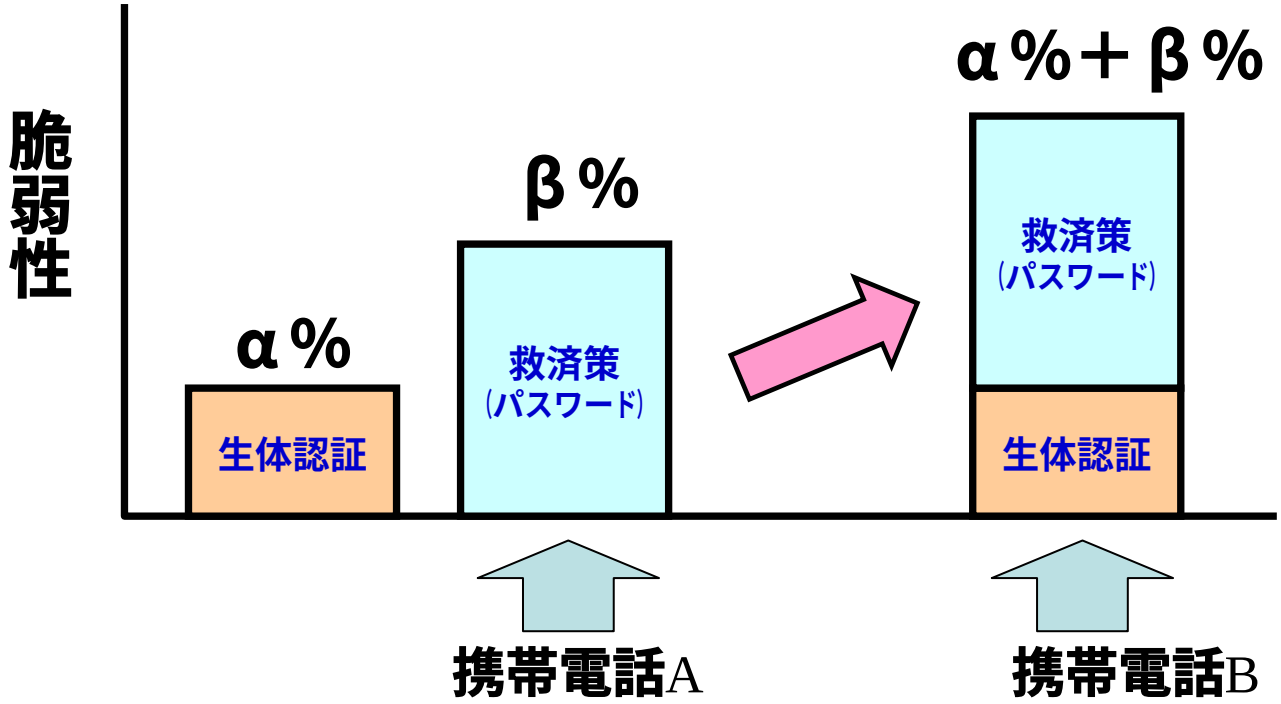
携帯電話B

脆弱性比較（セキュリティ強度）

パスワードだけ　ＶＳ．　救済用パスワードを併用する生体認証

生体認証・パスワード双方の脆弱性の合算値が全体の脆弱性（他人受容の確率）となる。

生体認証の脆弱性をα％としパスワードの脆弱性をβ％とすると、全体の脆弱性は（α＋β）％、つまりパスワードの脆弱性をβ％のままとすると、パスワード単独の脆弱性よりも大きくなる。



● 生体認証とパスワード併用と言いつつ利用者が生体認証機能をオフできる製品

パンフレット：

生体認証とパスワードのダブルロックを採用
セキュリティ機能がさらに充実！

取扱説明書：

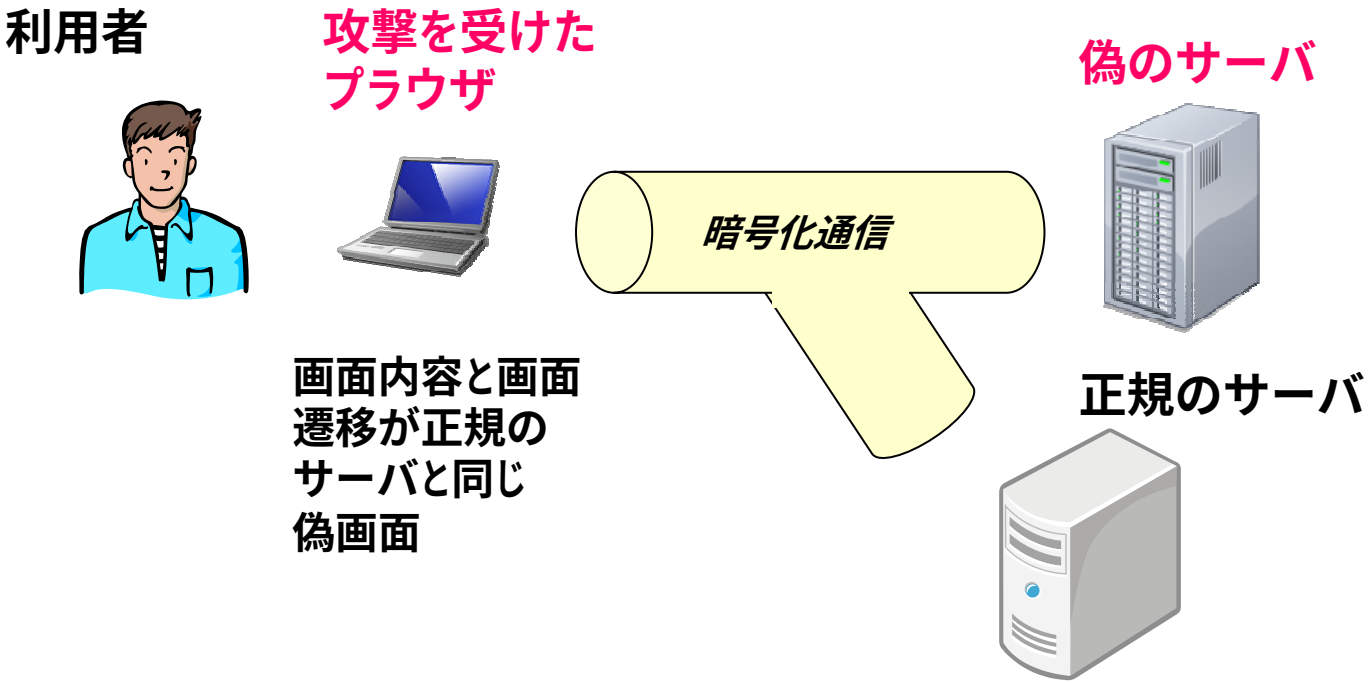
『生体認証キャンセル可能との旨』

が、灰色の小さい字で記載。

➡ パスワードだけで認証が可能となり、ダブルロックとは言えない状態に容易に陥る。

(5)　サーバ認証に関わる潜在的優良誤認

「正規サーバとの接続が確立した」旨の文章、アイコン、配色の変更で知らせる
メッセージの確認だけでサーバが本物であると安心しきってよいものか？



偽画面表示に対抗する何らかの手段が必要

これから重要なテーマとして顕在化してくると予想される

劣位誤認（安全・非安心）の例

劣位誤認とは，性能表示で述べている効用は存在し客観的に「安全」と評価できる本人認証技術にも拘わらず、その利用者は心持ちが「安心」して利用できないという構図

● 画像選択型本人認証

極端なケースにおける短所が全体的な弱点と見なされてしまう誤認例

- 数学的強度：表示画像数や登録画像数の小さなケースのみを取り上げる
- 覗き見　　：無警戒なユーザと特異性の目立つ画像表示のケースのみを取り上げる
- 推測攻撃　：ユーザの趣味や交友関係が推測されるケースのみを取り上げる

優良誤認や劣位誤認の原因発生

1. 本人認証技術の本質に関する理解不足
2. 製品･サービス提供側の不作為･注意欠如による情報発信
3. 不注意による情報発信のこだま現象
4. 製品･サービス側が誤解を恐れて正確に伝える努力をしていない
5. 利用者側の検証なしの思い込み

課題の取組み･解決の方向性提言

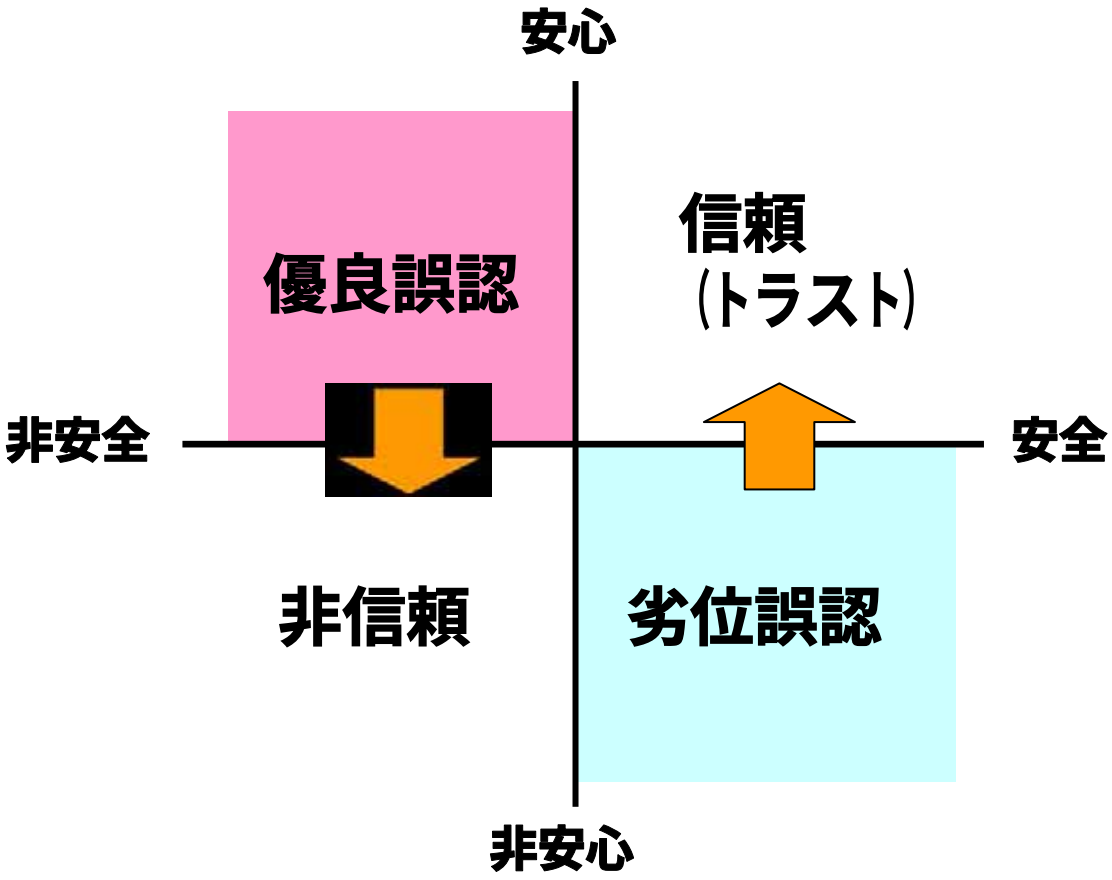
1．適正な表示のガイドラインの作成と普及

- リスクに応じた対応策ガイド
- 計画と適用のためのガイド
- 導入と運用のためのガイド

2．適正な情報の提供、利用者･消費者への啓発

- ガイドライン
- 情報提供
- 啓発

結び



実在すべきは「信頼」と「非信頼」の象限だけであって、他の2象限は常に空白状態となっていることが最も望ましい

- 「優良誤認」と「劣位誤認」は「信頼」への大きな障害である
- 「優良誤認」と「劣位誤認」を減少させることは「信頼」を高める
- 産官学メディアにより正しく適切な情報発信を行い国民を啓発
- **安全・安心なデジタル社会の定着に寄与**